Biometric Authentication and Authorization System for Grid Security

G. Jaspher Willsie Kathrine#, E. Kirubakaran*
#Department of Information Technology, Karunya University, Tamil Nadu, India
meet.katee@gmail.com
** DGM (Outsourcing), BHEL, Trichy, Tamil Nadu, India*
ekiru@bheltry.co.in

Abstract

Dynamicity in the data sharing has resulted in resource usage being more and more distributed and more open in nature. The need for problem solving and the distributed nature of data has resulted in the development of grid environment. Authentication is the first step of security requirement for any grid environment to validate the user. This paper proposes an authentication method which is depends on the password and the user ID along with the biometric data of the user and the geographic position of the user. The same biometric and position data used for authentication can be used for authorization purposes so as to reduce the cost and time of storing different data for different purposes. A Four-Factor based Privacy Preserving Biometric (4F2PB) authentication scheme for a grid environment is proposed which can work on the existing Network Framework. The proposed authentication scheme optimises the security required for the entry level user and prevents malicious user from entering into the grid environment.

Keywords: *Grid computing, authentication, virtual organisation, biometric data.*

1. Introduction

Grid computing involves sharing heterogeneous resources which are located in geographically distributed places belonging to different administrative domains [1]. Grid data sharing is not file exchange but rather access to computers, software, data and other resources. Grid involves the creation of a dynamic Virtual Organization (VO). Each virtual organization comprises of users and their resources and any other services (S) joined by a common goal [2]. Each of the user or resource is available from different administrative domains (DO). Each user or resource has its own trust policy which requires a local to global and global to local mapping of the access policies as discussed in [3].

The basic security for the Globus Toolkit (GT.0.2) is the Grid Security Infrastructure (GSI) in C [4][5]. It depends on the Public Key Infrastructure (PKI), X.509 Proxy certificates and TLS for authentication. GSI involves third party verification for authorization. The GSI security is secure enough but has scalability problems [5].

All of the existing security schemes are based on the user name and the password which belongs to a two factor authentication scheme. The proposed authentication scheme optimizes the security of a grid environment by adding more features like biometric data and the position of the user during and after authentication.

2. Related Work

User authentication has been in discussion for a long time to enhance the security of any system at the entry level itself. Many methods such as password based systems, ID based systems, etc have been used. A hash-chain based remote user authentication in which all the passwords are encoded is given in [6]. In all the initial remote based authentication systems, a verifier table is to be placed in the server side which becomes a problem if the server is compromised.

In order to avoid maintaining a verifier table Hwang et al., proposed a non-interactive smart card based scheme without verifier tables [7]. A finger print based remote user authentication scheme was proposed in [8]. This scheme was found to be vulnerable to masquerade attacks and many other attacks [9], [10]. In [11], [12], [13], the biometric data itself is taken as a key for encryption/decryption. The secret data is extracted by using the biometric template as the key. The biometric data is to be stored in the server side and used for comparison. But for effective Biometric authentication, the process is to be done in the client side [14] to avoid any problem due to the server being compromised [15]. In [16], the method has been optimized with the matching being done in the server side. But the server does not store any biometric data in its database thereby protecting the privacy of the user.

The method in [16] provides a three factor authentication which is password – something the user knows; smart card – something the user has; biometrics – something the user is. A further enhancement to this type of authentication is to add a fourth factor thereby providing a four factor authentication [17]. The fourth factor can be the addition of location of the user – someplace the user is. This fourth factor can be implemented by using the data obtained from the cookies of a user's web browser or computer or from the Global Positioning System (GPS) or the IP address location process. The fourth factor addition enhances the security criteria required for a vast distributed system such as a military or medical or research or Banking Grid environments. The military data sharing requirements take into consideration the place in which the user is positioned so as to find the location of any valid/invalid user. So, the sensitive areas of application require security with some amount of privacy preservation. By combining the biometric data with passwords and the location of the user, the security factors are further enhanced. The next section shows the methodology of the proposed Four-Factor based Privacy Preserving Biometric (4F2PB) authentication system.

3. Security Framework For A Grid System

The existing solution uses Open Grid Services Architecture (OGSA) architecture [18]. The OGSA architecture uses the WS-Security services for authentication and authorization. The existing system based on OGSA and GSI have some basic security solutions for solving the authentication and authorization criteria. The scalability, heterogeneity and increase in attack have led to the need of a new security framework which is based on the existing architecture with additional features to tackle the day to day attacks. The Co-operative Trustworthy Control Architecture for Computational Grids is shown in Figure 1. The main subcomponents of this proposed system in Figure 1 are,

a. A Security Client (SC)

b. A Security Manager (SM)

c. A Chief Security Manager (CSM)

Each grid environment in the given architecture has the following components:

Service (S) - Service/resource is the resource provider of the grid environment. Each resource provider can be a private individual or a member of another organization.

Service Policy (SP) – Every service holder has their own Service Policy based on the VO and the domain to which they belong. The service policy is based on the individual policy of the resource and the domain policy.

Domain (DO) – The Organization to which each individual service resides in is a Domain. It is not necessary that all the members of the same domain belong to the same VO. Every service decides on the VO's based on their own requirements.

Virtual Organization (VO) – A Virtual organization (VO) temporarily aggregates resources of different domains to achieve a common goal. It is considered as a highly-distributed, cross-domain computing infrastructure that is dedicated to supporting large scale resource sharing, resulting in dynamic collection of resource providers.

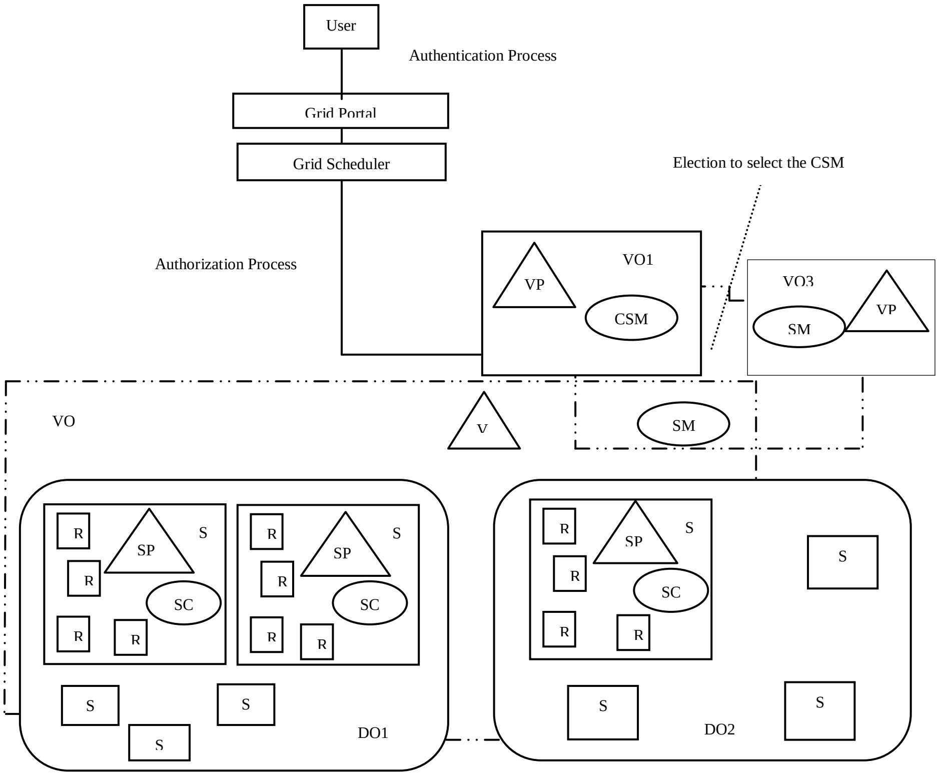


Figure 1. Co-operative Trustworthy Control Architecture for Computational Grid

Virtual Organization Policy (VP) – This is the policy set up of the VO which is followed by all the members of the VO. This policy is set based on a combination of the DO, SP, AuP, AuZP and OP. AuP is the authentication policy decided by the VO and AuZP is the authorization policy. Any other policy which is required cam be added in the Other Policy (OP). The policy setting determines the strength of the security.

The additional features added in the proposed architecture are the Security Client (SC) which is a security feature present within each service/resource of the Virtual Organization (VO). It is especially for the host level security. This security feature, will analyze/study the user requests and the processes for any impending security compromise. Once a compromise is identified, the detail is immediately sent to the VO's Security Manager (SM). The attack if any is then sent to the Chief Security Manager (CSM) which further analyses the input based on the audit log. IF any attack is identified by the CSM, it is informed to the various SM's of the other VO's to avoid the attack spreading further in the Gris environment.

4. Methodology of Four-Factor based Privacy Preserving Biometric authentication system

The Four-Factor based Privacy Preserving Biometric (4F2PB) authentication system four main phases such as the Initialization Phase, the Registration phase, the Login phase and the Mutual Authentication phase. An additional password change phase is added to ensure that the user can change his/her password when required. In each phase distinct operations are defined for the user and the server. The proposed authentication methodology is shown in fig.2.

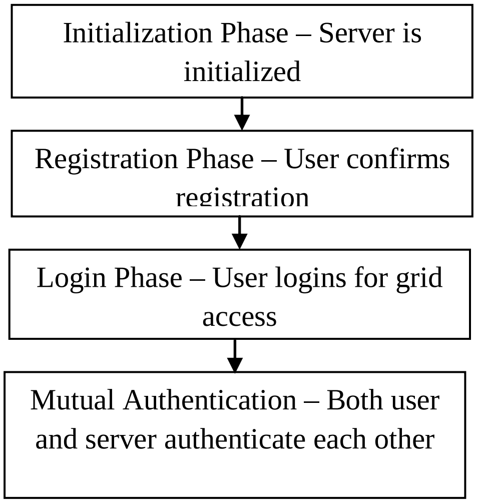

Initialization Phase – Server is initialized
Registration Phase – User confirms registration
Login Phase – User logins for grid access
Mutual Authentication – Both user and server authenticate each other

Figure 2. 4F2PB Authentication Methodology

The initialization phase is done in the server side for each user which may join in the grid network. In the Registration phase based on the details provided by the user along with the inputs given by the server, the smart card data is stored and given to the user through a secure medium. Only during the Login and the mutual authentication phase is the user and the server authenticated to each other. Once the mutual authentication is a success, then the user can go on to the next operation involved in the data transaction. The triple DES along with any other light-weight encryption algorithm can be used. The process flow of the 4F2PB authentication scheme is shown in fig. 3.

During the initialization phase, the server stores both the asymmetric and symmetric key in its database. Once a user requests for registration, the server accepts the user's hashed biometric data and the password in a secure way. This way assures that the server does not know the actual biometric data and neither is biometric data stored in any database within the server. The validity of the user is checked based on the comparison of the hashed biometric data rather than the original data. This method of storage makes sure that the user's data is not lost under any circumstance.

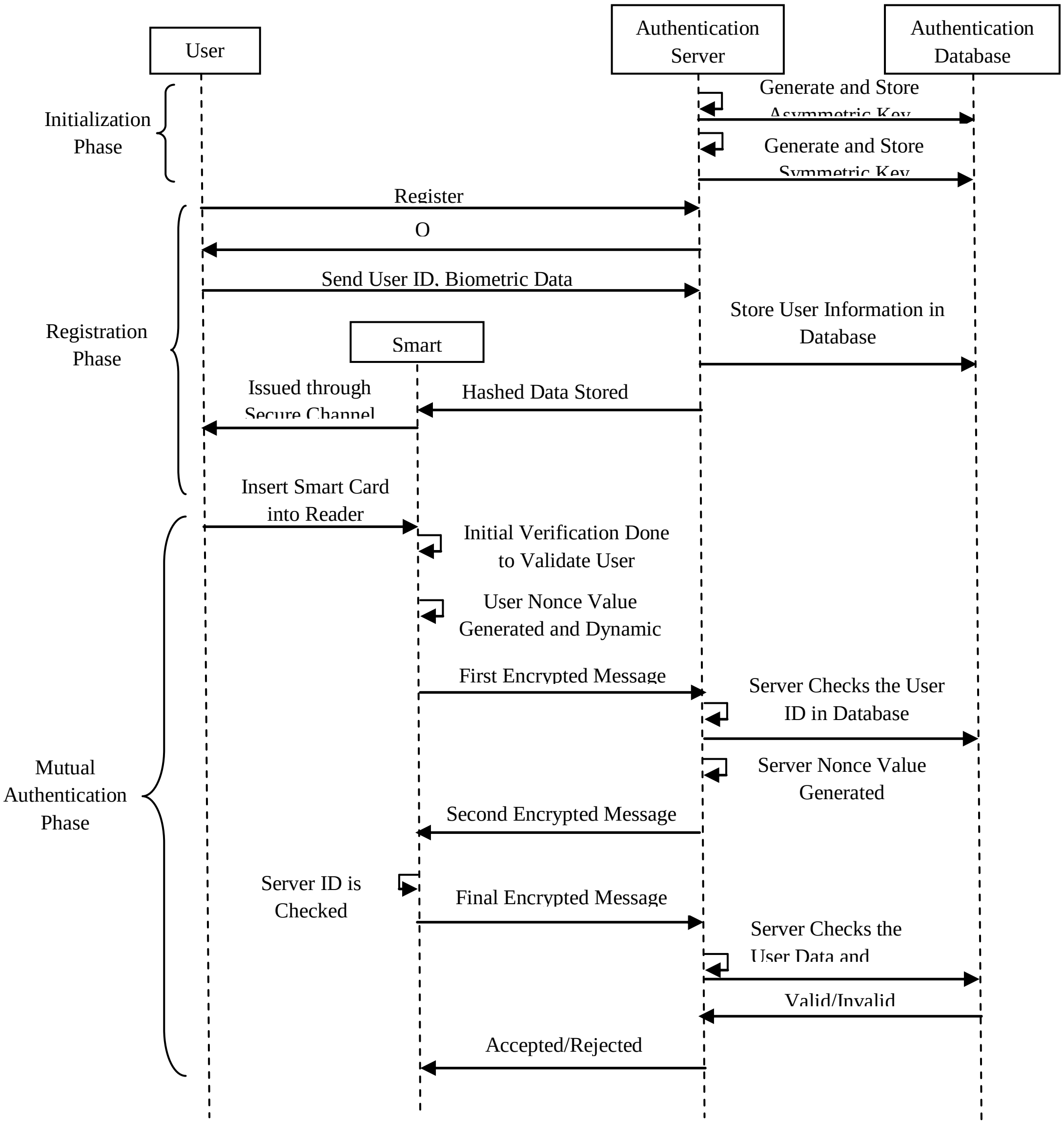

User
Authentication Server
Authentication Database
Initialization Phase
Generate and Store Asymmetric Key
Generate and Store Symmetric Key
Registration Phase
Register
O
Send User ID, Biometric Data
Store User Information in Database
Smart
Issued through Secure Channel
Hashed Data Stored
Insert Smart Card into Reader
Initial Verification Done to Validate User
User Nonce Value Generated and Dynamic
First Encrypted Message
Server Checks the User ID in Database
Mutual Authentication Phase
Server Nonce Value Generated
Second Encrypted Message
Server ID is Checked
Final Encrypted Message
Server Checks the User Data and
Valid/Invalid
Accepted/Rejected

Figure 3. Process of the Proposal 4F2PB Authentication Scheme

All the hashed data are stored in the server's database and the encrypted data required for the further use of the user is stored in the smart card and sent to the user. The user then uses the smart card for further access to the Grid environment. The smart card does the initial validation of the user and then forwards the user data to the server, where further authentication is the done. In the proposed scheme, both the user and the server validate each other and hence it is complete mutual authentication. Only when the user and the server both satisfy the validation criteria then the data transfer occurs. If the user validation does not succeed it is rejected or the user is requested to start the authentication from the beginning of the login phase. The next section gives the detailed explanation of each phase of the 4F2PB authentication system.

5. Four-Factor based Privacy Preserving Biometric Authentication System

Biometric Authentication (BA) of every grid member can be used to enhance the security of the grid environment. The biometric authentication involves using a smart card which holds the data of what the user is i.e., the biometric data such as finger print, iris, etc, what the user knows i.e., the password (PW) and the data that the user has i.e., Identifier (ID). The 4F2PB method has four phases such as Initialization phase, Registration Phase, Login phase and a password change phase. The first three phases are based on the authentication scheme described in [16] with some additional features. The added features are the dynamic User ID (CID), the dynamic server ID (SID) and the position location feature for the user (pos_i) and the server (pos_s). The server supports symmetric and asymmetric encryption and decryption. The notations used in this paper are given in Table 1.

Table 1. Notations used in this Paper

S_i	Server
U_i	User
S_{ID}	Identity of Server S_i
ID_i	Identity of User U_i
B_i	Biometric data of U_i
(PW_i)	Password of U_i
$h(.)$	One-way hash function
x	The master secret key
(p_k, s_k)	Public-private key pair
$\oplus$	The Exclusive-OR Operation
$\|\|$	Message Concatenation
r	Random Number generated by U_i
n_u	Nonce value generated by U_i
n_s	Nonce value generated by the server S_i
pos_i	Position of the user U_i
pos_s	Position of the server S_i

5.1 Initialization Phase

During the initialization phase, the server generates a public-private key pair. The server also generates a secret key for symmetric encryption and decryption. The server keeps the private key and the secret key secure.

The following are the series of steps done in the Initialization phase:

a. Server generates public-private key pair (p_k, s_k) for asymmetric encryption/decryption.

b. Server generates a secret key x for symmetric encryption/decryption.

c. Both (x, s_k) is kept secure in the server.

5.2 Registration Phase

During the registration phase, the user tries to register for a grid membership within a Virtual Organization (VO). During the membership registration, the user is given a particular Identifier(ID_i). The user registers his/her biometric data (B_i) which maybe a fingerprint or an iris template. The user also selects a random number r and a password(PW_i) .

The operations done at the user side are:

a. The user records his/her user Identifier (ID_i)

b. The user records the biometric template (B_i)

c. The user selects a random string r and password (PW_i)

The user computes $SB_i = \delta(B_i) = h(r \oplus B_i)$ .The value of SB_i is sent to the server securely along with the one-way hash function $h(.)$ of the Password and the ID of the user. The server receives $(ID_i, h(PW_i), SB_i)$ through a secure channel. By using the values sent by the user, the server computes, y_i such that,

$$y_i = E_x(ID_i \parallel h(PW_i) \parallel SB_i) \qquad \text{--------------} \quad (1)$$

where $E_x(.)$ represents the symmetric encryption using the secret key x.

The operations continued in the server side are:

a. Server computes $K = h(ID_i \parallel x)$

b. Server stores $(K, y_i, h(.), p_k)$ in the smart card.

c. Server sends smart card to the user securely.

Once the user receives the smart card, a few entries are to be stored in it along with the data already available in the smart card i.e., y_i.

The following operations are done to confirm the registration:

a. The user enters the biometric data which can be an iris data /fingerprint B_i

b. The user encrypts the random number r with B_i such that $E_{B_i}(r)$ is obtained.

c. $E_{B_i}(r)$ is stored in the smart card.

d. $SB_i = \delta(B_i) = h(r \oplus B_i)$ is stored in the smart card.

5.3 Login Phase

A user U_i is allowed to enter the grid environment using his/her smart card. The user enters his/her Password $(PW)'$ and does a biometric scan denoted by B_i^*. The user's smart card retrieves the random value "r" from $E_{B_i}(r)$ by using the biometric data $B_i^{'}$ entered by the user U_i. The smart card computes $SB_i{}^* = \delta\,(SB_i^{'}) = h(\,r\,\oplus B_i^{'})$. This value is compared with the already stored value of $SB_i = \delta\,(B_i) = h(\,r\,\oplus B_i)$ to confirm if the user is the same. Then the smart card generates a nonce value "n_u" and computes $M = (K \oplus n_u)$. Then CID_i is calculated such that, $CID_i = h(ID_i \parallel n_u)$

Then value of C_0 is computed such that,

$$C_0 = E_{pk}\,(M \parallel CID_i \parallel y_i \parallel u \parallel pos_i) \qquad \text{------------} \ (2)$$

Where $E_{pk}(.)$denotes the encryption function using the server's public key. "u" is the random value selected by the user during login time. pos_i - denotes the position at which the user is during this phase.

To ensure the liveliness of the user, a nonce value is added in the value of C_0 along with the already existing random values to add more security. C_0 is sent to the server.

5.4 Mutual Authentication Phase

Once C_0 is received by the server, the server does the following operations,

a. Server decrypts C_0 using its private key s_k

b. Server computes "n_u^*" such that $n_u^* = M \oplus K$ where $K = h(ID_i \parallel x)$

c. The validity of the user is checked by using the Identifier ID_i to the one received by the server. By using the value of n_u^* the value of CID_i^* is calculated.

d. Then the value of CID_i^* is compared with the value of $CID_i$to check if $CID_i = CID_i^*$.

e. Also the value of ID_i can be verified with the ID stored in the ID table for the users at the server end. A comparison of ID's is done to make sure that verification is done correctly even when the Server ID table is corrupted.

f. The remaining terms of C_0 i.e.,$(h\,(PW_i) \parallel SB_i)$ is retained for future reference.

Server computes a values of C_1 such that

$$C_1 = E_u\,(N \parallel SED \parallel S_{ID} \parallel v \parallel pos_s) \ \text{--------------} \ (3)$$

Where S_{ID} = Server's identity and v is the random number chosen by the server and u is the random number selected by the user and sent in C_0. The server generates a nonce value "n_s" and computes $N = (K \oplus n_s)$. pos_s denotes the position of where the server is during the authentication session and Server ID $SED = h(S_{ID} \parallel n_s)$. This is done to make sure that the data was not tampered during transmission. Server sends C_1 to the user U_i.

In the User Side, the following operations are done,

a. The smart card decrypts C_1 using the random value of u.

b. The value of S_{ID} is checked for valid server ID. The smart card computes $SED^* = h(S_{ID} \parallel n_s^*)$ using its nonce value n_s^*. Smart Card computes "n_s^*" such that $n_s^* = N \oplus K$ where $K = h(ID_i \parallel x)$.

c. Then SED^* is calculated by using the value of the generated n_s^* and ID_i., i.e., $SED^* = h(S_{ID} \parallel n_s^*)$. If $SED^* = SED$, then the server is valid and the data has not been tampered with.

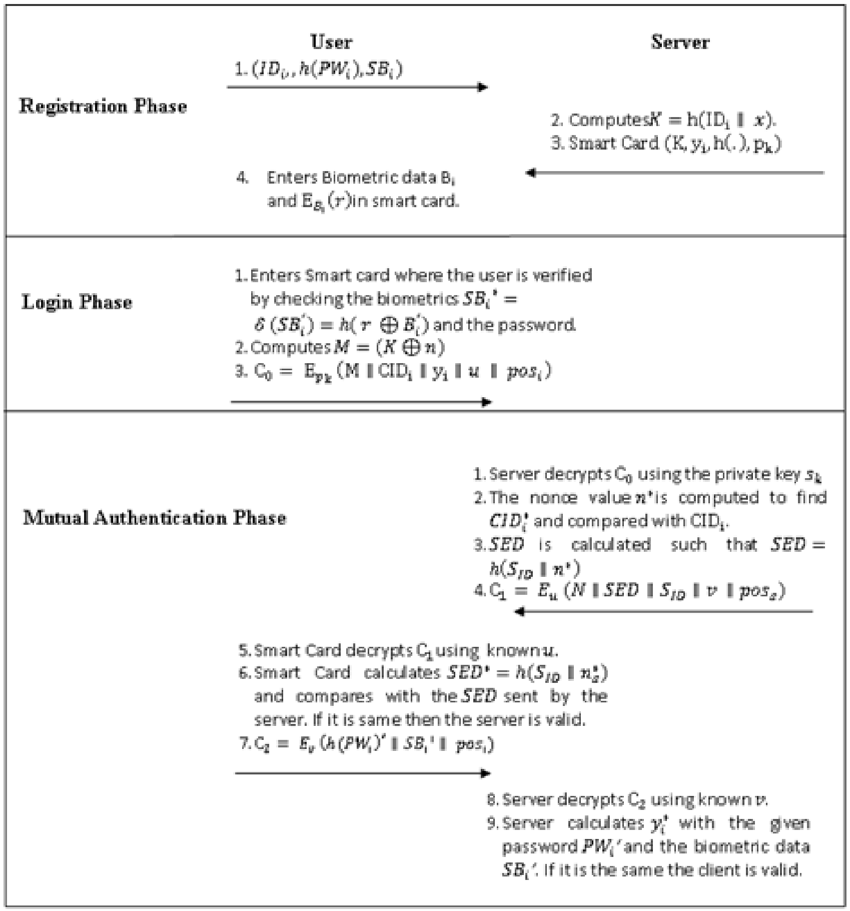
d. The position of the server is stored by the user for further use.

The smart card calculates the following value

$$C_2 = E_v\,(h(PW_i)' \parallel SB_i' \parallel pos_i) \text{ ----------------------} \qquad (4)$$

Where pos_i denotes the position at which the user is during this instant.

The server decrypts C_2 using v and calculates the value of y_i^* from the values sent in C_2 . If $y_i^* = y_i$, the server matches the values of the password and the biometric template to confirm the authenticity of the user. Finally, the server checks the position of the user.



Registration Phase

1. $(ID_i, h(PW_i), SB_i)$
2. Computes $K = h(ID_i \parallel x)$.
3. Smart Card $(K, y_i, h(.), p_k)$
4. Enters Biometric data B_i and $E_{B_i}(r)$ in smart card.

Login Phase

1. Enters Smart card where the user is verified by checking the biometrics $SB_i' = \delta(SB_i') = h(r \oplus B_i')$ and the password.
2. Computes $M = (K \oplus n)$
3. $C_0 = E_{pk}(M \parallel CID_i \parallel y_i \parallel u \parallel pos_i)$

Mutual Authentication Phase

1. Server decrypts C_0 using the private key s_k
2. The nonce value n' is computed to find CID_i' and compared with CID_i.
3. SED is calculated such that $SED = h(S_{ID} \parallel n')$
4. $C_1 = E_u(N \parallel SED \parallel S_{ID} \parallel v \parallel pos_s)$
5. Smart Card decrypts C_1 using known u.
6. Smart Card calculates $SED' = h(S_{ID} \parallel n_s^*)$ and compares with the SED sent by the server. If it is same then the server is valid.
7. $C_2 = E_v(h(PW_i)' \parallel SB_i' \parallel pos_i)$
8. Server decrypts C_2 using known v.
9. Server calculates y_i^* with the given password PW_i' and the biometric data SB_i'. If it is the same the client is valid.

Figure 4. Proposed 4F2PB Authentication Scheme

The position of the user cannot change drastically between C_0 and C_2 thereby indicating to the server that there is no presence of an attacker. If an attacker is to attack, he/she has to position themselves in the in the correct position and the nonce all in once which makes the attack much difficult. The value of SB_i^* in C_2 is compared with SB_i of y_i. If the value match is within a threshold range then the user is confirmed valid. The flow of the proposed scheme 4F2PB is shown in fig. 4. The main phases three phases are considered for computing the cost since they will be used repeatedly. Once all the steps in fig.4 have been completed successfully, it is clear that mutual authentication of both the user and the server is done for login of the user. The server secret number v can be used as a session key material and $h(v)$ can be used as a session key which is shared with the server.

5.5 Password Change Phase

The user U_i is authenticated by using the Password (PW') used initially for login process. Once authenticated, the user is prompted to enter the new password. Once the new password (PW'') is entered, the $y_i = E_x(ID_i \| h(PW_i) \| SB_i)$ value of $h(PW_i)$ is replaced with the value of $h(PW_i'')$. Thereby the user is allowed to further login by using the new password. The next section gives a brief discussion on the security analysis of the 4F2PB authentication scheme.

6. Security Analysis of the 4F2PB Authentication Method

In this section, the security and performance analysis of the 4F2PB authentication scheme are presented. The attacks which are withstood by the proposed scheme of authentication is explained.

6.1 ID-Theft Attack

As in equation $C_0 = E_{pk}(M \| CID_i \| y_i \| u \| pos_i)$, a dynamic user ID named as CID_i is created by the smart card based on the nonce value $n_u$instead of using the user's own ID. This helps to withstand the ID-theft attack and also preserves the privacy of the user.

6.2 Clock Synchronization and Replay Attack Problem

In [19], the problem in timestamp based authentication is given as replay attack due to the transmission delays in an unpredictable network. Even though the networks are fast the speed may vary based on the geographical and political distribution. To avoid using of timestamps, a nonce value n_u is used each time the user sends his/her data and a nonce value n_s is also used by the sever to proclaim the server's validity. Since a nonce value such as n_u and n_s in equations $C_0 = E_{pk}(M \| CID_i \| y_i \| u \| pos_i)$ where $M = (K \oplus n_u)$and $C_1 = E_u(N \| SED \| S_{ID} \| v \| pos_s)$ where $N = (K \oplus n_s)$ can be used only once, and not repeated, the user/server can be safeguard themselves from replay attacks.

6.3 Modification Attack

Each authentication message in from equation (1), (2), (3) and (4) include a one-way hash function along with an encryption algorithm. The hash value in each equation requires a nonce value or a random value. Even if the attacker gets hold of each of these equations the decryption part and breaking the hash function is not possible. If the attacker has the value of

$h(PW_i)$, to find the password, the attacker needs find an equivalent of the hash function by trying each password. This attack is difficult because the attacker has to first break into the encrypted data $C_0 = E_{pk}(M \parallel CID_i \parallel y_i \parallel u \parallel pos_i)$. The attacker then needs to send the correct dynamic ID using the nonce and the position value pos_i. For an attacker to get all the values correct is impossible which makes modification attack difficult. Without knowing the actual data of these two values, the original data cannot be modified. Modification of the equations will be noted by the legitimate user and server and since all the messages are linked, it makes modification attack harder.

6.4 Mutual Authentication

At the end of the mutual authentication phase, both the server and the client authenticate each other thereby establishing mutual authentication. During each phase, of the equations C_0, C_1 and C_3, the user and server check the validity of each other using the values of CID, SED, M, N and the position data's. If the server has any doubt in the validity of the user, the message C_2 can be asked to be resent and the position can be checked.

6.5 Man-in-the-middle Attack

An attacker A who tries to do a man-in-the middle attack needs to know the decryption keys u, v and r in each message signal else its message will be discarded by the server or the client. The position data pos which is considered as the fourth factor is to be within a threshold for the final authentication to hold valid.

6.6 Security of the Stored Data on the Smart Card

The smart card holds the value of $(ID_i, y_i, h(.), p_k)$ where, $y_i = E_x(ID_i \parallel h(PW_i) \parallel SB_i)$. If the smart card is compromised, the data it provides is not easily accessible to the attacker. Without knowing the matching password and the ID of the user, the attacker cannot move further along the authentication phase. Knowing the public key of the server complicates matters since the attacker has to find the encryption algorithm and a matching value of C_0 to send to the server. Furthermore, the hash function has to be broken in order to get the secret data. The biometric data is stored in the open for anyone to copy it. It is stored in the form of a template combined with a random string which needs to be found to get the data. Thus the data stored in the smart card is secure.

7. Performance and Functionality Analysis of the 4F2PB Authentication Scheme

In this section, the performance and functionality of the 4F2PB authentication scheme is analysed and comparison has been made with the X. Li et al. scheme and Li and Hwang scheme. Where T_h denotes the time complexity of the one-way hash function and T_{EN} is the time taken to complete one full Encryption algorithm. In [20], X. Li et al. have provided a comparison of their biometric remote authentication system and Li and Hwang scheme [21] of authentication. The 4F2PB authentication scheme proposed in this paper is compared with the X. Li et al. scheme and Li and Hwang scheme as shown in Table 2.

Table 2. Performance Comparison of the 4F2PB Scheme with Other Biometric Schemes

Phase	4F2PB Scheme	X. Li et al. Scheme [20]	Li and Hwang Scheme [21]
Initialization Phase	Server Initialized	No	No
Registration Phase	$1T_{EN}+2T_h$	$4T_h$	$3T_h$
Login Phase	$1T_{EN}+1T_h$	$4T_h$	$2T_h$
Mutual Authentication Phase	$3T_{EN}+2T_h$	$7T_h$	$5T_h$
Total	$5T_{EN}+5T_h$	$15T_h$	$10T_h$

The Table 2 has been generated based on the time taken for each phase. The Registration phase involves the time taken for two has function and one encryption algorithm; the login phase involves the time taken for one hash function and one encryption algorithm and the Mutual Authentication phase has a total time taken as a combination of three encryption operations and two hash functions. The overall time taken to complete the 4F2PB scheme of authentication is much less when compared to the existing biometric authentication systems. This is an added advantage of the 4F2PB authentication scheme.

The Table 3 gives the overall security comparison for X. Li et al. scheme and Li and Hwang scheme with our proposed 4F2PB algorithm. The 4F2PB includes an initialization phase whereas [20],[21] do not propose such a phase. The four factor algorithm takes a much lesser time with more security when compared with X. Li et al. scheme and Li and Hwang scheme. Since a dynamic ID is used for the user with a combination of a nonce value, the 4F2PB algorithm resists ID-theft attack whereas X. Li et al. scheme and Li and Hwang scheme use the ID of the user and hence are vulnerable to such attacks.

Table 3. Security Comparison of the 4F2PB Scheme with other Biometric Schemes

Factors	4F2PB scheme	X. Li et al. Scheme [20]	Li and Hwang Scheme [21]
Computational Cost	Low($5T_{EN}+5T_h$)	Low ($15T_h$)	Low ($10T_h$)
Mutual Authentication	Yes	Yes	No
Resistance to replay attack	Yes	Yes	Yes
Resistance to modification	Yes	Yes	No
Resistance to man-in-the-middle attacks	Yes	Yes	No
Factors in Authentication	4	3	3
Matching Biometric data in remote server	Yes	No	No
Resist ID theft	Yes	No	No

The biometric matching is not done mostly in the smart card in 4F2PB but rather in the remote server without losing the privacy of the biometric data. The Exclusive OR operation requires less computational time thereby cost when compared to the hash function and encryption operations and hence the cost of it is neglected. Any light-weight public-key cryptosystem can be used for the encryption and decryption process.

8. Authorization Scheme Using Biometric Data

Authorization involves primarily the process of providing the access control to the users for the resources. Access Control in our architecture is based on Role Based Access Control (RBAC) [22]. For providing RBAC, some sets of policies are to be formulated for the Grid Environment and the corresponding virtual organizations. The policies are formulated based on the combination of the Domain policy to which the user is a part, the VO policy of which the user is a member and the user's own requirements. RBAC is implemented using the XACML/SAML for appropriate access details.

The access control is implemented by the collaboration between the policy decision points (PDPs) and policy enforcement points (PEPs). PDPs perform authorization decisions; whereas PEPs carry out the access decisions made by the PDPs. In this security architecture, PDP's are the Security Manager and PEP's are the Security Clients. The service policy of this security architecture consists of a combination of the Domain Policy (DO), Resource Policy (RP) and any Other Policies (OP) pertaining to the resource (OP_R). The Authentication Policy (AuP) and Authorization Policy (AuZP) are formulated in the Virtual Organization Policy set (VP). The final effect of the policy is either a Permit a Deny. Some further access policies like specifying which all parts of the services or resources can be permitted rather than giving a denial can also be added.

Fig. 5 gives the combined structure Authentication and Access Control mechanism for which can be added for this architecture.

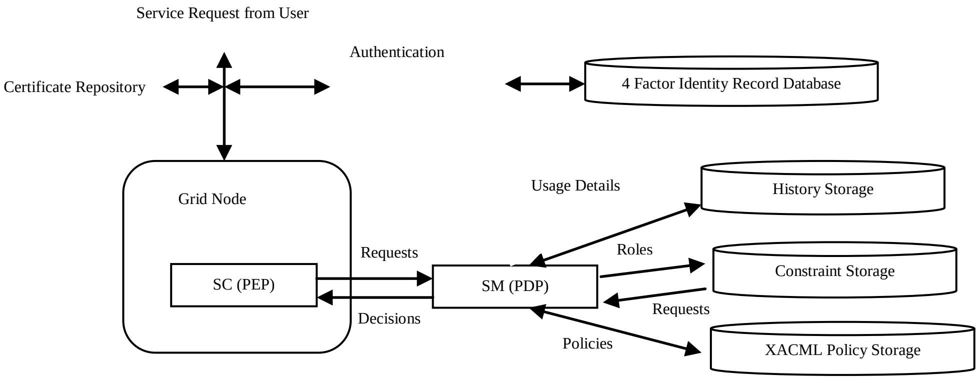


Figure 5. Authorization Scheme Combined with the Authentication Scheme

The SC and the SM communicate through a secure channel. The SM decides on the access decisions based on the policy set of the VO and the RBAC details of the user. The user's previous history along with the user's present requirements decides the access criteria for the user. The details are stored for future use. This further enhances providing the access to the user.

In the Fig.5, the PEP and the PDP are the Security Client and the Security Manager of proposed architecture. As in Fig.5, the user gets authenticated to enter into the grid environment. After authentication to access any resource or service, the user's viability is finalized with the roles provided to the user, his /her usage history and the policyset of the service. The biometric data of the user is linked with his/her roles for access of the required resource [23]. The resource access is based on the policy set of the resource provider and the rights provided to the user.

9. Conclusion and Future Work

The proposed Four-Factor based Privacy Preserving Biometric authentication scheme has provided an enhanced security with an optimal overall time taken for the operation. The scheme provides a four factor authentication with better security prospects for any user in the grid network. By increasing the security during the authentication phase itself we can try to minimize any other malicious insider attacks and also reduce external attacks. The biometric data used for authentication can also be used in the consecutive authorization process thereby lessening the database space utilized by reusing the data used in authentication. A further study in the analysis of the biometric authorization is to be done to check for its viability.

References

[1] Ian Foster, "What is the Grid? A Three Point Checklist", 2002.

[2] Foster, C. Kesselman, S. Tuecke, "The anatomy of the grid: enabling scalable virtual organizations", Int. J. High Performance Computing, 2001.

[3] Quan Zhou, Geng Yang, Jiangang Shen, Chunming Rong, "A Scalable Architecture for Grid", Sixth International Conference on Parallel and Distributed Computing, Applications and Technologies, 2005.

[4] Bendahmane, M. Essaaidi, A. El Moussaoui, A. Younes, "Grid Computing Security Mechanisms: State-of-The-Art", International Conference on Multimedia Computing and systems ICMS '09, pp535-540, 2009.

[5] http://www.globus.org/toolkit/docs/4.0/security/GT4-GSI-Overview.pdf

[6] L. Lamport, "Password Authentication with insecure Communication", ACM Communications 24(11), 770-772, 1981.

[7] T. Hwang, Y. Chen, C.S. Laih, "Non-Interactive password authentication without password tables", IEEE Conference on Computer and Communication Systems, pp. 429-431.

[8] J.K.Lee, S.R.Ryu and K.Y.Yoo, "Fingerprint-based remote user authentication scheme using smart cards", Electron. Lett., vol.38, no.12, pp.554-555, 2002.

[9] C.C.Chang and I.C.Lin, "Remarks on fingerprint-based remote user authentication scheme using smart cards", ACM SIGOPS operating System Rev., vol.38,no.4, pp. 91-96, 2004.

[10] C.H.Lin and Y.Y.Lai, "A flexible biometrics remote user authentication scheme", Computer Standards Interfaces, vol.27, no.1, pp.19-23, 2004.

[11] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric cryptosystems: Issues and challenges," Proc. IEEE, Special Issue on Multimedia Security for Digital Rights Management, vol. 92, no. 6, pp. 948–960, Jun. 2004.

[12] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data", in Eurocrypt 2004, pp. 523–540.

[13] A. Juels and M. Wattenberg, "A fuzzy commitment scheme", in Proc. ACMConf. Computer and Communications Security, 1999, pp. 28–36.

[14] Y. Sutcu, Q. Li, and N. Memon, "Protecting biometric templates with sketch: Theory and practice", IEEE Trans. Inf. Forensics Security, vol. 2, no. 3, pp. 503–512, Sep. 2007.

[15] C.M. Chen and W.C. Ku, "Stolen-verifier attack on two new strong-password authentication protocol", IEICE transactions on Communications, E85-B (11), 20002, pp. 2519-2521.

[16] Chun-I Fan and Yi-Hui Lin, "Provably secure remote Truly Three-Factor Authentication Scheme with Privacy Protection on Biometrics", IEEE Transactions on information Forensic and Security, vol. 4, No.4, December 2009.

[17] http://blog.dustintrammell.com/2008/11/21/four-factor-authentication

[18] http://www.ogf.org/documents/GFD.80.pdf

[19] L. Gong, "Security risk of depending on synchronized clocks", ACM Operating System Review", ACM Operating System Review. 26(1), pp. 49-53.

[20] Xiong Li, Jian-Wei Niu, Jian Ma, Wen-Dong Wang, Cheng-Lian Liu, "Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart cards", Journal of Network and Computer Applications 34 (2011) pp.73-79.

[21] Li C-T, Hwang M-S," An Efficient biometrics-based remote user authentication scheme using smart cards", Journal of Network and Computer Applications, 2010, 33(1) pp. 1-5.

[22] D.F. Ferraiolo, R. Sandhu, S.Gavrila, "Proposed NIST standard for role-based access control. ACM Transactions on Information and System Security", 2001, 4(3): 224 – 274.

[23] Bechara Al Bouna, Richard Chbeir, Stefania Marrara, "Enforcing role based access control model with multimedia signatures", Journal of Systems Architecture 55 (2009) 264–274.

Authors

Jaspher W. Kathrine received the B.E degree in Electrical and Electronics from Bharathiyar University and the M.E degree in Computer Science and Engineering from Anna University. She is currently working towards her Ph.D. degree in Computer Science and Engineering at Karunya University, Coimbatore, India. Her primary research interests include network security, key management, biometric security features and grid security. She is a professional body member of IAENG, IACSIT and ISTE. She is a reviewer of Journal of Network and Computer Applications and International Journal of Computer Theory and Engineering (IJCTE).

Dr. E. Kirubakaran obtained B.E (Hons.) degree in Mechanical Engineering, M.E. in Computer Science and Ph.D. in Computer from Regional Engineering College, Tiruchirappalli. He has obtained his M.B.A. degree from IGNOU. He has more than 30 years of Industrial experience at Bharat Heavy Electricals Ltd. Tiruchirappalli and presently he is employed as Senior Deputy General Manager at BHEL. He has been a visiting faculty to a number of educational institutions. He had held the posts of Secretary, Vice-Chairman and Chairman of Computer Society of India, Tiruchirappalli. He is a Member of the Syndicate of Bharathidasan University, Member in the Academic Council Anna University, Trichy and Academic Council Anna University, Chennai.